



3 1176 00156 0193

DOE/NASA/20305-79/3  
NASA TM-79193

NASA-TM-79193 19790020554

NASA TM-79193

# **SAFETY CONSIDERATIONS IN THE DESIGN AND OPERATION OF LARGE WIND TURBINES**

Dwight H. Reilly  
National Aeronautics and Space Administration  
Lewis Research Center

June 1979

**LIBRARY COPY**

JUN 1979

LANGLEY RESEARCH CENTER  
LIBRARY, NASA  
HAMPTON, VIRGINIA

Prepared for  
**U.S. DEPARTMENT OF ENERGY**  
**Energy Technology**  
**Distributed Solar Technology Division**



NF00505

#### NOTICE

This report was prepared to document work sponsored by the United States Government. Neither the United States nor its agent, the United States Department of Energy, nor any Federal employees, nor any of their contractors, subcontractors or their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product or process disclosed, or represents that its use would not infringe privately owned rights

SAFETY CONSIDERATIONS IN THE  
DESIGN AND OPERATION OF  
LARGE WIND TURBINES

Dwight H. Reilly  
National Aeronautics and Space Administration  
Lewis Research Center  
Cleveland, Ohio 44135

June 1979

Work performed for  
U. S. DEPARTMENT OF ENERGY  
Energy Technology  
Distributed Solar Technology Division  
Washington, D. C. 20545  
Under Interagency Agreement DE-AI01-79ET20305

## TABLE OF CONTENTS

	<u>Page</u>
INTRODUCTION . . . . .	1
SYSTEM DESCRIPTION . . . . .	2
Program Objectives . . . . .	2
System Configuration and Operation . . . . .	2
Deployment . . . . .	3
SYSTEM SAFETY REQUIREMENTS AND PROGRAM IMPLEMENTATION . . . . .	3
SAFETY APPROACH, ANALYSIS AND VERIFICATION . . . . .	5
Environment . . . . .	6
Operating Profile . . . . .	6
Load Calculations . . . . .	6
Allowables and Safety Margins . . . . .	8
Structure Member Sizing . . . . .	9
Fail Safe, Safe Life and Product Assurance . . . . .	9
Preliminary Design . . . . .	10
Detail Design . . . . .	12
Fabrication, Installation and Acceptance . . . . .	12
MOD-2 SAFETY SYSTEMS . . . . .	14
CONCLUSION . . . . .	16

# SAFETY CONSIDERATIONS IN THE DESIGN AND OPERATION OF LARGE WIND TURBINES

by Dwight H. Reilly

National Aeronautics and Space Administration  
Lewis Research Center  
Cleveland, Ohio

## INTRODUCTION

The objective of the Federal Wind Energy Program is to accelerate the development of economical wind energy systems so that wind energy will become a viable technological alternative to other forms of energy. To achieve this objective requires advancing the technology as well as addressing the non-technological issues which, if not understood and planned for, could deter the use of wind energy. The primary challenge for the designer of wind turbines is production of a low cost wind energy system that operates unattended, is reliable, is relatively maintenance free, and is environmentally acceptable. In meeting this challenge, the designer is faced with multiple design requirements which must be satisfied during the design process. Among the most important of these requirements is system safety. From the outset of the program the designer must address, in a formal and disciplined way, the issues associated with safety of hardware, safety of the environment and above all safety of the public and the construction and maintenance personnel.

The Department of Energy and NASA are currently engaged in the development of several large wind turbines ranging in rated power from 100 kilowatts to multi-megawatt output. Safety has been a primary consideration in all of these wind turbine developments.

The safety methodology and disciplined approach to design is best exemplified in complex aircraft and space programs which have safely transported man to the moon. This approach embodies a program where all functions, design, fabrication, assembly, checkout, and operation, are controlled by formal procedures, rigorous design reviews, and the close scrutiny of independent safety, reliability, and quality organizations.

Modern wind turbines are a combination of centuries old windmill technology, standard commercial practices of the electric power and steel construction industry, and advanced aerospace technologies related to helicopter rotors, computer analyses, materials, etc. As such wind turbine generators should be relatively hazard free and cost effective if the safety techniques developed in the aerospace industry are applied in a judicious and systematic manner while recognizing both the unique and standard commercial characteristics of these devices.

The process used to assure safety in the design and operation of large wind turbines utilizing the Mod-2 wind turbine as an illustrative example is described herein.

## SYSTEM DESCRIPTION

Program Objectives. - The Department of Energy, the NASA Lewis Research Center and the Boeing Engineering and Construction Company are engaged jointly in the development of a 2500 kW wind turbine system (WTS) designated as the MOD-2 WTS. The goal of the MOD-2 project is to produce a wind powered electrical generating system for utility applications which will be economically competitive with conventional power generating equipment. The program started in August of 1977 and the first unit will be installed and operating by mid-1980. The MOD-2 is representative of large wind turbines and as such will be used herein to describe "typical" configurations.

System Configuration and Operation. - Figures 1 and 2 illustrate the MOD-2 overall dimensions and layout. It has a rotor diameter of 300 feet with the center of rotation 200 feet above the ground. The configuration embodies several advanced concepts such as a teetering up-wind rotor, partial span pitch control, light-weight gearbox and low natural frequency tower; all specifically selected to minimize the cost of electricity.

The WTS begins to generate power at wind speeds above 14 mph (as measured at the hub), and rated power of 2500 kW is generated at wind speeds between 27.5 and 45 mph. It is structurally designed to withstand wind speeds up to 120 mph measured at 30 feet above ground level.

The tower is approximately 193 feet tall and is composed of a 150 foot long, 10 foot diameter cylindrical tube, and a flared tower section which has a diameter of 21 feet at its base. The tower is attached to the foundation with anchor bolts. The type of foundation used will depend on soil conditions (in typical soil conditions a buried octagonal stepped foundation of reinforced concrete will be used).

A transformer and the bus tie contactor unit are located outside of the tower base. All other control equipment is located within the tower base. The utility's electrical interface is at a fused manual disconnect switch located on the tower.

The equipment layout within the nacelle is illustrated in Figure 3. Personnel access is via a lift within the tower. Exceptionally heavy equipment may be transferred to and from the nacelle through top hatches. Smaller loads can be hoisted from the ground by a monorail that extends beyond the aft end of the nacelle or by the man-lift. The lift stops at a deck inside the tower below the nacelle floor. Final access is by means

of a ladder from the deck up into the nacelle. A fire detection and extinguishing system, emergency exits and non-powered emergency man-lowering devices are provided at each end of the nacelle.

The electrical power system consists of the electrical equipment required for generation, conditioning, and distribution of electrical power within the WTS. Electrical power at appropriate voltage is delivered at a utility interface point which is the output side of a fused manual disconnect switch located at the foot of the tower. Once the WTS and the utility are electrically connected, the existence of the tie automatically results in generator voltage and frequency control, and thus maintains constant generator and rotor rpm.

Normal operations are as follows: When the WTS is shut down but in a ready-for-operation condition, i.e., in the standby mode, the rotor and yaw brakes are on. The control system initiates start-up whenever the hub height average wind speeds are between 14 and 42 mph at the hub. For start-up, the yaw brake is released, the nacelle is yawed so as to align the rotor with the wind, blade pitch is moved from the feathered to the breakaway position, the rotor brake is released, and the rotor starts rotation.

In the normal operating mode and with the wind speed below rated wind, the pitch angle is scheduled to deliver maximum power. Above rated wind speed the pitch angle is controlled to maintain constant rated power.

The WTS is shutdown when wind speeds become too low.

For normal shutdown, the control system causes the blades to be feathered, and disconnects the generator from the utility when power drops below 125 kW. The rotor teeter brake is applied and when the rotor stops rotation, the rotor brake is applied to prevent inadvertent rotation, all pumps are turned off, and the WTS automatically enters the standby mode.

Deployment. - The MOD-2 WTS is designed to be used by electrical utilities either singly or in multi-unit farms, with the output tied into the utility grid. Operation is unattended although status information is supplied to the utility substation via a CRT. A keyboard at the utility substation enables the utility operator to interrogate the micro-processor located in the WTS nacelle. This capability allows the utility operator to determine the WTS operating condition, current output and limited diagnostic information.

#### SYSTEM SAFETY REQUIREMENTS AND PROGRAM IMPLEMENTATION

The DOE/NASA wind energy office has required that contractors make safety considerations an integral part of all phases of the wind turbine programs. The following are excerpts from the MOD-2 contract.

## System Safety

1. The Contractor shall provide a System Safety Plan (as a part of the product assurance program plan) for the development, fabrication, transportation, erection and operational phases of the program. WT safety program reviews shall be conducted as part of the scheduled overall design and/or program review to assess the status of compliance with the overall safety program objectives.
2. Safety analyses shall be performed and shall specifically encompass the following areas of safety:

- a. Operational Safety

The WT design shall be such that one failure or any malfunction causing performance degradation shall not create a hazardous or catastrophic condition by reason of its mode of failure, or by the direct effect of such failure on the WT equipment, or personnel.

- b. Other Safety

Installation, transportation, and maintenance procedures shall minimize human error or failure of equipment, injury to personnel, and damage to the WT. Mechanisms involved shall be designed to eliminate or minimize hazards to personnel in areas where maintenance will be performed.

Responding to these requirements, the MOD-2 Product Assurance Plan describes how safety disciplines are integrated into the program and describes the specific safety analyses and reviews that are to be accomplished. The introduction to the safety section states:

The wind turbine safety program will identify, evaluate and either eliminate or control all undesired system events (hazards) with the potential to:

- a. cause loss of program objectives
- b. injure personnel
- c. damage system or support equipment and facilities

These objectives will be accomplished by identifying the equipment, functions and operations that may result in hazards, assessing those hazards for impact and probability, by instituting methods to eliminate hazards or reduce hazards to an acceptable risk, and to verify implementation of control measures in design, operating controls and procedures for installation, test and maintenance.



Hazard Analysis. - Hazard analysis identifies hazards inherent in designs and subsystem operations, assesses hazard impact and probability, and identifies safety requirements to eliminate hazards or reduce hazards to an acceptable risk. Safety requirements include:

- a. Design and procedural constraints.
- b. Requirements for safety devices and warning methods.
- c. Special procedures, protective equipment and personnel training.

The plan goes on to further define these elements and to explain how the hazard analyses and design reviews will be conducted and corrective actions taken where needed. Figure 4, taken from the MOD-2 Safety Plan, illustrates this process.

Initial construction, testing and on-going maintenance activities can pose problems commonly associated with industrial safety. The MOD-2 program ensures compliance with Occupational Safety and Health Act (OSHA), State, NASA and Boeing requirements, and has charged line management with the prime responsibility for enforcing daily compliance with established safety standards. Audits are performed to ensure that the safety plan is adequately implemented in all operational areas and any deficiencies, corrective action and/or follow-up actions taken are recorded and maintained on file.

Specific safety plans are developed to address the safety considerations associated with the site activation, erection and test phases of the program.

As the development of the WTS progresses from the conceptual and preliminary design phases, the overall design approach to safety and the solutions to specific potential safety problems are established. These are incorporated into the program specifications. Figure 5 depicts the development process and how safety considerations are factored into the program. The following section describes how each of the elements shown in Figure 5 are implemented.

#### SAFETY APPROACH, ANALYSIS AND VERIFICATION

Figure 6 illustrates the disciplines used to assure the safety of the MOD-2 WTS. The approach used is to produce a safe-line design (i.e., that the structure sustain no failure during its service life) and then to provide a means of safely stopping the WTS should a failure occur. This "fail safe" philosophy provides a back-up safety system both for maintenance personnel and to prevent major damage to the WTS. Following is a discussion of each major element shown in Figure 6.

Environment. - Large wind turbines could be deployed in a wide variety of locations and physical environments. In order to assure that the MOD-2 will be capable of safely operating in these environments, all elements of the system are designed to meet the environmental criteria specified in Figure 7. The values specified in this figure are based on research by both NASA/DOE and The Boeing Company and represent conditions that are applicable to potential WTS sites.

Operating Profile. - In order to compute the structural loads that the WTS must safely carry, it is necessary to calculate the load spectra that the WTS components will be subjected to over the 30 year life. For each revolution of the rotor, the blade structure experiences a cyclic reversal of chordwise bending loads due to gravity (1 per rev loads) and cyclic air loads due to the variation of wind speed with height above the ground at a rate of two per rev loads. These load variations also experience the effects of wind gusts. In addition, the components experience the loading variations of each startup and shutdown cycle. The one and two per rev loads over the 30 year WTS life represent 200 and 400 million cycles respectively. The number of cycles and the corresponding causes of startup/shutdown are as follows:

21,900	low wind speed shutdowns
1,500	high wind speed shutdowns
180	planned shutdowns for maintenance
725	unplanned shutdowns for maintenance/spurious faults
<u>24,355</u>	

These cycle frequencies are based on analysis of the wind spectra and a detailed reliability/maintainability analysis of all of the system components. As added conservatism to assure safe-life design, the above cycles are increased by a factor of three to 73,000 cycles. It is also expected that the WTS will experience some partial but incomplete startups at marginally low wind speeds. The structural fatigue life therefore conservatively assumes an additional 73,000 cycles up to one-half of the operating cyclic stress levels. All cyclic loading contributes to structural fatigue stresses in the WTS. Although the startup/shutdown cycles are relatively few, their stress magnitudes are high and contribute most significantly to fatigue life.

Load Calculations. - Loads are calculated based upon the natural and induced environments defined in the previous subsection. A brief description of the major considerations associated with the loading condition calculations follow:

- o Limit Operating Loads - Maximum operating loads result from extreme gustiness during normal operation in which the nacelle is at a yaw angle within  $\pm 20$  degrees of the mean wind direction. The limit operating load is the maximum 99.99 percentile calculated load.
- o Operating Fault Loads
  - o Overspeed - 115 percent of normal

- o Inadvertent blade feathering - caused by loss of hydraulic pressure, faulty actuator or servo control.
- o Inadvertent rotor, yaw and teeter braking - caused by inadvertent loss of hydraulic pressure, faulty actuators or control system.
- o Hazard Load Conditions - During operation, the WTS must withstand structural loads due to seismic disturbances, projectile impact, transportation and handling, lightning, hail, and temperature extremes.
  - o Seismic - The WTS, excluding the foundation, will withstand seismic disturbances characteristic of Zone 3. The foundation shall be designed to seismic disturbances and soil conditions appropriate to the site.
  - o Projectile Impact - The blades, nacelle and tower are designed to withstand impact of 4 lb. projectile at 35 mph (or equivalent momentum) without structural failure. This loading condition could come from bird impact, objects propelled by the wind, etc.
  - o Transportation and Handling - The WTS components and shipping containers are designed to sustain the transportation environment in Figure 7. These conditions conservatively cover all of the environments anticipated during transportation throughout most of the U.S.
  - o Lightning - The WTS must withstand lightning strikes without structural damage. (The characteristics of lightning strikes are defined in the MOD-2 System Specification.)
  - o Hail - During operation, the WTS must withstand structural damage the impact of 1.0 inch diameter hail stones (50 pc density) with 66.6 ft. per second terminal velocity.
  - o Temperature Extremes - The WTS is designed to operate in the temperature range of  $-40^{\circ}$  F to  $+120^{\circ}$  F.
- o Non-operating Load Conditions - The extreme environmental loading conditions which are considered for the WTS in the parked configuration are extreme wind, snow and ice.
  - o Extreme Winds - The MOD-2 WTS is designed to withstand loads associated with a maximum steady wind of 120 MPH at the 30 ft. reference elevation. The WTS shall withstand the design maximum wind with the rotor parked and braked in any position.
  - o Snow - WTS structural components are designed to withstand 21 lb/sq ft. of snow on the rotor blade when parked horizontally and 41 lb/sq ft. of snow on the nacelle roof.

- o Ice - WTS structural components are designed to withstand 2.0 in. of glaze ice (with density of 60 lb/ft<sup>3</sup>) on all exposed surfaces.

Although the loads are analytically calculated, the analytical models were verified by wind tunnel tests using 1/20th scale models, and full scale static buckling tests.

Allowables and Safety Margins. - With all the loading conditions established, the capability of the selected structural materials to withstand all loading conditions is then determined. Extensive structural testing is performed on typical structural sections to verify the allowable stresses. Buckling tests are performed to confirm the allowable buckling stresses at the maximum loads and cyclic fatigue tests are performed to establish the allowable stresses which preclude failure over the 30 year life. Further assurance is provided by safety factors applied to the design limit loads. These factors of safety are defined as follows:

(a) Factors of Safety

Factors of safety shall be applied only to loads and pressures. They shall not be applied to heating rates, temperatures, thermal stresses and deformations, or any other environmental phenomenon unless otherwise specified.

(b) Limit Load Factor

There shall be no buckling, yielding or permanent deformation of structure under design limit loads obtained when the following safety factors are applied to the limit load described in Section 4.0.

Hoisting and handling	3.0
All other conditions	1.0

Pressure vessels, lines and fittings shall withstand maximum operating pressure or relief valve pressure setting, whichever is greater, multiplied by the following safety factors to preclude yielding:

Hydraulic Systems	2.0
Pneumatic Systems	2.5

(c) Ultimate Load Factor

There shall be no ultimate failures under the design ultimate loads obtained when the following safety factors are applied to the limit loads described in Section 4.0.

Hoisting and Handling Loads	5.0
Rotor Blade Buckling	1.35
All other conditions	1.25

Pressure vessels, lines and fittings shall withstand maximum operating pressure or relief valve pressure setting, whichever is greater, multiplied by the following safety factors to preclude bursting:

Hydraulic Systems	4.0
Pneumatic Systems	5.0

(d) Casting Factors

A minimum casting factor of 2.0 shall be applied to the design load factors for all castings.

(e) Fitting and Lug Factors

In addition to the foregoing factors, a fitting factor of 1.15 shall be applied to design loads for all fittings. This factor shall apply to all portions of the fitting, the means of attachment of the fitting and the bearing stresses of the members joined. In the case of integral fittings the part shall be treated as a fitting up to the point where the section properties become typical of the member. This factor does not apply to standard structural steel connections designed in accordance with AISC specifications.

(f) Tower Overturning

The foundation shall be designed so that no uplift occurs at any point on the base for any design load condition, when the structure is founded on a yielding base. All base materials except solid rock and hard shale shall be considered as yielding. A safety factor against overturning of not less than 1.5 shall be used when comparing dead load resisting moment with live load overturning moment taken about the toe of the foundation. Where the structure is founded on solid rock or hard shale the above requirement against uplift need not be met; however, a minimum safety factor against overturning of 2.5 shall be used.

Structural Member Sizing. - Structural member sizing is accomplished by a disciplined multi-point analysis of all the loading conditions and corresponding allowables. The analysis recognizes all the potential combinations of loading conditions and the number of occurrences during the system life of 30 years. Although structural sizing with its applied factors of safety is a well understood technology, the calculations and the design details are verified for critical components by structural test of full scale hardware as indicated in figure 6.

Fail-Safe, Safe Life and Product Assurance. - Fail-safe is a design concept that requires the component or structure to fail in such a way that either adequate warning is given the operator that a failure is pending so corrective action can be initiated, or the design automatically places the machine in a safe operating mode or is shutdown.

Mechanical and electrical components are designed such that failure of these parts result in safe shutdown. Where this is not possible, redundant components are considered to keep the machine in an operating

mode while the operator is warned through automatic devices. The maintenance program provides assurance that the redundancy has not been lost. Use of redundant circuit paths, relays, etc. on critical systems where failure could result in rotor overspeed is particularly important.

For structural components fail-safe requires that the structure be capable of sustaining detectable damage (fatigue or other) for a reasonable time between inspections without catastrophic failure. To achieve this concept, multiple load paths are provided in the structure, or a failure detecting system is required.

For the MOD-2 program, all parts of the structure not designed to fail-safe strength criteria meet a safe-life strength criteria. Safe-life is a structural concept which require that the structure sustain no failure during its service life. To achieve this concept, use is made of load factors and/or factors of safety during design. These additional factors of safety may be achieved by reducing the allowable working stress to a level that is low enough to preclude crack propagations to failure. MOD-2 hardware is designed to the safe-life concept when high cost or weight penalties prevent use of the fail-safe concept. To obtain safe-life design, hardware elements or components have load-time histories established for their expected service life and have service life analysis including fatigue analysis and tests conducted to verify adequate life.

Product assurance plans and procedures are an integral part of those activities assuring the safety of the WTS. The Statement of Work and Contractor Product Assurance Plan for the MOD-2 program recognize both the unique and standard commercial characteristics of the machine. Where unique or critical components, procedures or practices are involved, more stringent controls are invoked. Critical forgings or blade material, as an example, may be traced from the original melt or rolling process. Requirements are relaxed, however, to allow cost effective use of standard "off the shelf hardware" possible.

Whether unique or standard, the test, inspection, and acceptance procedures and criteria for each component and each process in the fabrication and assembly of the WTS are defined. The reject or repair of components or processes such as a weld which fails to pass the quality acceptance criteria is controlled by disciplined record procedures. These data are documented and reviewed for proof of completion at the "readiness" reviews which precede each of the major program milestones such as site installation, first rotation, and turnover to the operating utility. Details of the product assurance/inspection function are discussed in the section related to hardware fabrication, installation, and acceptance testing.

Preliminary Design. - With the foregoing data, structural members are sized and the preliminary design is established. This preliminary design is then subjected to critical review by all the staff technical disciplines.

An integral part of the preliminary design process is the conduct of a failure mode and effect analyses (FMEA), wherein all possible failure modes are identified, their effects analyzed and corrective actions taken as appropriate to preclude undesirable consequences. The FMEA's are completed by the cognizant designers and reviewed by system engineers and a reliability specialist. The failure severity code used in the analysis is described in Table 1 and an example of a completed FMEA is shown in Figure 8.

Completion of the FMEA's by the designers as an in-line part of the design process resulted in numerous design changes to either prevent serious failure modes or reduce their impact. Whenever applicable, failure frequency data was included in the analyses to quantify the probability of occurrences.

The failure frequency data used to quantify the failure mode frequencies was developed as part of a comprehensive reliability/maintainability analyses conducted during conceptual and preliminary design. Extensive research was conducted to accurately estimate the expected Mod-2 component failure rates. This analysis was conducted on all of the WTS elements, including major items such as the generator and gearbox, and smaller component parts (e.g., switches, connectors, sensors etc.). The failure rate data was taken directly from utility field experience whenever such data was available. For components not normally used in the utility industry (e.g., hydraulic actuators) applicable commercial experience was used. In developing the failure rates, actual hands-on experience was used in lieu of theoretical predictive data thus providing a more realistic appraisal of the expected field experience.

Over 750 failure modes were analyzed and numerous corrective actions were implemented to preclude costly failures. Special attention was directed at all potentially catastrophic failure modes. The results of this effort are summarized in Table 2. Two examples from the failure mode analyses which affected design are discussed below:

- (1) Potential failure modes such as control linkage binding, bearing failures, or hydraulic control failures are not catastrophic because redundancy is now built into these systems. As shown in Figure 9, each blade tip and associated control linkage operates off an independent hydraulic actuator system. Redundancy in these systems and their associated control sensors assures that a failure in either system does not affect the other. In addition the WTS can be brought to a safe stop by feathering one tip even though the opposing tip has been driven to the worse case high power position.
- (2) Use of A633 low alloy steel in the WTS blades required that consideration be given to development of a crack detection system to provide warning of the presence of a potentially damaging fatigue crack or equivalent damage anywhere in the outer surface of the rotor. The system developed is shown in Figure 10. A continuous flow of pressurized air is provided to each blade. The flow rate to each blade is electronically compared. Any unbalance between the two flows causes the crack detection system to signal the WTC control system to feather the blade tips and shut the machine down before any significant rotor damage occurs.

In addition to directly affecting the design of the WTG, the FMEA is a valuable tool in developing checkout, inspection and maintenance

requirements and procedures. During the preliminary design phase, components critical to the fail-safe philosophy are identified. Special attention is given these items during assembly, checkout and maintenance to assure redundant design features are available and active during the life of the hardware and hardware with single point failure modes are adequately inspected and maintained to minimize the probability of the single point failure.

Preliminary design is concluded with an extensive "readiness" review by NASA. This review assures that all required and planned analyses, including safety analyses, have been satisfactorily completed and that the preliminary design meets all requirements. The NASA then authorizes the program to proceed into the detail design phase.

Detail Design. - During the detail design phase the approved preliminary design is further developed into detail drawings which can be released for fabrication. During this period all of the staff disciplines again review and analyze all details of the design. All of the plans, procedures, criteria, and specifications, including maintenance plans and equipment, safety plans, product assurance plans, etc., are finalized. During this period, the total configuration is placed under rigid configuration control. Any proposed design change must undergo a disciplined review by all technologies to assess the impact of a change on all elements of the program. The design change could impact maintenance procedures, safety, fabrication processes, product assurance inspection requirements, structural integrity, etc. Only after thorough evaluation indicates the change to be favorable will a change be authorized. The NASA reviews all changes and must provide approval to proceed on all significant changes which affect form, fit, function or contractual specification requirements

The detail design phase concludes with an intensive "readiness review" by the NASA. This review assures that the detail design meets all requirements. The DOE/NASA can then authorize the program to proceed with hardware fabrication, assembly, functional test, installation and checkout, and acceptance testing.

Fabrication, Installation and Acceptance. - This is a critical phase of the WTS program which must assure that the WTS is built to the design configuration, that it is built with the specified quality, and that testing verifies that the system meets all requirements. The significant responsibility during these activities lies with the Product Assurance Organization. As previously discussed, extensive plans and requirements for quality have been documented and disciplined processes and procedures established. Inspection and test of each detail is monitored per the planned procedures and accepted or rejected per the established criteria. Each process, function, and component hardware is verified to be within specification. For example, product assurance procedures and requirements for the materials and structures of the Mod-2 WTS include destructive and non-destructive testing.



These tests verify that the materials and built up structure of the WTS meet the design requirements. Destructive tests on representative samples of material include:

- (1) chemical analysis,
- (2) static strength, including yield and ultimate tensile strengths,
- (3) charpy V-notch impact test at -40° F.

In addition, ultrasonic (non-destructive) testing of representative material samples is planned. Specific weld inspections are specified on the design drawings. For example, the current Mod-2 plans require visual, penetrant, radiographic and ultrasonic inspection of critical blade welds.

All testing is performed per the approved Mod-2 test plan in a sequential manner that verifies product integrity and system safety prior to proceeding to the next step. The verification testing starts with functional checkout and test of the system assemblies prior to transporting to the WTS site. This testing assures that no unplanned event could cause a safety hazard during erection, test or operation of the WTS. It also assures that all functions are properly interfaced and that all systems including the control system hardware and software function per all of the specification requirements.

Sequential testing during installation and checkout assures system integrity and system safety prior to subsequent installation events. For example, following erection of the tower, and prior to installation of the nacelle, safety related tests such as the following are planned to assure product integrity and readiness for nacelle installation:

- (1) Continuity test of installed electrical circuits.
- (2) High potential tests of power transmission circuits.
- (3) Bus tie contacted function test.
- (4) Accessory power distribution and control.
- (5) Operation of nacelle access device.
- (6) Operation of tower man-lift.
- (7) Alignment and functional check of nacelle and drive train components.
- (8) Functional check of mechanical equipment and the electrical/electronic control system components.

With the system completely installed and all functional testing including fail-safe verification completed, a "readiness review" will be conducted. Satisfactory completion of this review will authorize initial wind powered rotation. Initial rotation will be performed at wind velocities between 15 and 20 mph. The WTS will be initially operated at 8 rpm using manual controls. During this operation, all test data will be closely monitored to verify that the data system is completely operative and that structural dynamic coupling is as predicted. When it is verified that the WTS is operating as predicted at 8 rpm, further rotational testing will be initiated at 17.5 rpm at wind velocities less than 20 mph. Initial rotation at 17.5 rpm will be with the synchronizer enable command inhibited. This will allow verification of phase rotation and other tests such as automatic control system functions and the ability to perform automatic shutdown. With successful completion of these planned tests, the WTS will be operated in synchronization with the utility network. After complete verification testing and demonstration in all operating modes at all wind speeds, and completion of user training, the system will be approved by NASA for turnover to the operating utility company.

The foregoing discussion of sequential testing has illustrated the planned discipline which will result in an inherently safe system. To assure safety during fabrication, installation and testing, the manufacturing plan, the test plan, and the product assurance plan have specific sections devoted to procedures for safety of personnel. A safety engineer is assigned for daily monitoring of personnel safety systems and procedures. To assure safety of the utility maintenance personnel, a system maintenance manual including safety procedures is delivered with the WTS. The training program for construction, test and maintenance personnel is a contractual requirement.

The following section describes the significant features which are being designed into the Mod-2 WTS to enhance personnel safety.

## MOD-2 SAFETY SYSTEMS

The previous sections of this document have explained how safety issues are specified in the initial contracts, expanded in the project specifications and implemented in the design. This section presents the results of these efforts on the Mod-2 WTS.

The Mod-2 Safety design is summarized as follows:

- o All structural elements are designed to last for the life of the system (Safe-Life design)
  - o Loads calculated
  - o Safety Factors added
  - o Tests conducted to reduce uncertainty
    - o Strengths of materials
    - o Loads

- o Microprocessor control system constantly monitors WTS condition and shuts the system down upon failure of a primary device or a monitoring device.
  - o Orderly shutdown when failures occur
  - o Open circuits cause shutdown (i.e., signals from sensors) normally "hot" so that microprocessor sees closed loop)
- o Independent, redundant safety sensors and shutdown system incorporated
- o Full protection for electrical equipment
- o Compliance with Occupational Safety and Health Act and other applicable construction codes.
- o Gross hazards and failure modes and effects analysis conducted resulting in numerous additional safety features.

The approach to achieving system integrity has been previously discussed. The following is a brief discussion of the control system which schedules the on-going WTS operation and implements the failsafe actions to shutdown the WTS should faults occur.

The control system provides the sensing, computation, and commands necessary for unattended operation of the WTS as shown in Figure 11. The controller is a microprocessor which is located in the nacelle control unit and initiates start-up of the WTS when the wind speed is within prescribed limits. After start-up, it computes blade pitch and nacelle yaw commands to maximize the power output for varying wind conditions. Continuous monitoring of wind conditions, rpm, power and equipment status is also provided by the microprocessor which will shut down the WTS for out-of-tolerance conditions.

A control panel and CRT terminal are located in the tower base to provide operating and fault data displays and manual control during maintenance. A remote CRT terminal at the utility substation will provide display and limited WTS controls.

The WTS is protected from computer system failures by an independent back-up failsafe shutdown system. The failsafe system provides sensor redundancy on critical components, and initiates shutdown independent of the primary control system when necessary. A failsafe philosophy is used for all equipment condition signals, wherein presence of a voltage is an indication of a "good" signal. Thus, should a wire or connection to or from a sensor open, the WTS will detect a loss of voltage and shutdown the WTS. Figure 12 lists the signals monitored by both the normal control system and the independent back-up failsafe system.

The WTS electrical power system, Figure 13, employs a four pole synchronous generator containing an integral brushless exciter. Excitation control is provided to maintain proper voltage prior to synchronization with the utility and to provide a constant power factor output afterwards. Protective relays are provided to guard against potential electrical faults, out-of-tolerance performance, or equipment failures. These relays detect over-voltage, loss of excitation, under-frequency, overcurrent, reverse phase sequence, reverse power and differential current, and will protect the system by inhibiting synchronization, directing the control system to shut down, or if required, tripping the generator circuit breaker, resulting in a high speed shutdown. The generator is protected by overtemperature sensors on the forward and aft bearings and in the windings.

Power is delivered to the utility transmission line through a bus tie contactor. Its operation is controlled by automatic synchronization equipment which is both redundant and failsafe. Accessory power for operation, control and maintenance is obtained from the utility or from the generator output depending on the operating mode, and is internally conditioned to appropriate voltage levels. A battery, floating across a charger, provides an uninterruptable power supply for operation of protective devices and critical loads.

The major reasons for incorporating the safety features discussed above are: (1) to ensure that the public will not be injured by WTS failures and (2) to minimize damage to the WTS in the event of hardware failures. In addition to these considerations, the WTS must provide a safe environment for the conduct of scheduled and unscheduled maintenance activities. All components must be accessible and must be installed such that they can be removed and replaced without imposing hazards to maintenance personnel. The Mod-2 WTS complies with all applicable OSHA requirements and has used MIL-STD-1472, "Human Engineering Design Criteria for Military Systems, Equipment and Facilities," as a design guide. These design criteria, as well as the general design goals discussed previously are summarized in Figure 14.

In addition to the "design for safety" criteria shown in Figure 14, it is necessary to incorporate back-up personnel safety systems such as emergency egress doors, and escape devices. Conduct of the gross hazards analysis results in the identification of such additional safety features. These features, along with several others discussed previously, are summarized in Figure 15.





## CONCLUSION

The modern wind turbine is a unique marriage of the procedures, practices, and technology developed and used by the utility, construction and aerospace industries. Development of wind energy as an acceptable, low cost energy source requires wind energy systems demonstrate reliable, safe operation. The safety assurance program


evolved for these systems makes use of the lessons learned from these industries and the safety, reliability, and quality assurance tools developed by them.


The operational safety of wind turbines is directly related to the prevention of rotor overspeed and structural failures of major components such as blades, hub, drive train and tower. These failure modes are aggravated by the variable environment to which the machine is subjected, the inherent dynamic characteristics of the machine, and the need to operate and maintain the system with a minimum of on-site operator monitoring and control.

To meet these challenges, an engineering and safety program has been developed that involves a careful definition of the WTS natural and operating environments, use of well proven structural design criteria and analysis techniques, an awareness of potential hazards via the FMEA and gross hazards analysis, and use of a failsafe and redundant component engineering philosophy. It is expected that this program, when coupled to an effective quality assurance and system checkout program, will demonstrate that wind energy systems such as Mod-2 will meet the safety and reliability objectives of the DOE/NASA Large Wind Turbine Program.

Hazard category	Impact			
	Function	Repair cost	Time to repair	Personnel injury
Minimal	None 	and Under \$1,000	and Under 2 days	and None
Marginal	None critical 	and Under \$1,000	and Under 2 days	and First aid
Critical	Loss of function 	or Up to \$10,000	or Up to 10 Days	or Hospital
Catastrophic	Loss of system 	or Over \$10,000	or Over 10 days	or Fatal or permanent disable

 Minor items that can be repaired with convenience.

 No loss of generating capability, but repair must be accomplished within 2 weeks to avoid shutdown.

 Causes WTS shutdown.

 Destruction of major element such as rotor or gear box.

Table 1, FMEA Safety and Failure Severity Category Guide

Table 2, Summary of Major Failures and Effects – MOD-2-107

Failure	Effect	Corrective action
<b>Structural failures</b>		
<b>Rotor</b> <ul style="list-style-type: none"> <li>• Ice forms and is thrown off</li> <li>• Blade fatigue cracks</li> <li>• Spar buckling</li> <li>• Fatigue crack at control tip spindle end thread or at tip-blade interface</li> <li>• Inboard joint-rotor to hub bolt or flange weld failure</li> <li>• Broken teeter trunnion or flange cracks</li> <li>• Buckling inboard sections or hub compression skins</li> </ul>	<p>Could injure public – remote possibility Loss of part of rotor and possible secondary damage if allowed to progress</p>	<p>Ice detection system added Crack detection system shuts down WTS prior to incurring serious damage Safe life design Fatigue tests Inspection schedule Mid-blade assembly buckling test</p>
<b>Drive</b> <ul style="list-style-type: none"> <li>• Broken low speed shaft</li> <li>• Broken quill shaft bulkhead joint</li> <li>• Teeter shaft or flange cracks</li> </ul>	<p>Loss of load</p> <p>Possible extensive rotor damage</p>	<p>Emergency shutdown effected prior to reaching damaging overspeed Safe life design Strain gage correlation Safe life design</p>
<b>Tower</b> <ul style="list-style-type: none"> <li>• Failure of structure or foundation</li> </ul>	Extensive damage	Safe life design
<b>Control system failures</b>		
<ul style="list-style-type: none"> <li>• Signal to one tip incorrectly drives control surface to zero pitch</li> <li>• Control linkage to one tip jams</li> <li>• Control system signal to both pitch actuators incorrectly drives control surfaces to zero pitch</li> <li>• Power output sensor fails, calling for power increase when system is already at full power output</li> </ul>	<p>Emergency shutdown triggered by differential of tip position signals</p> <p>Emergency shutdown triggered by generator output power sensor</p> <p>Damaging overspeed possible if load drops off prior to initiating shutdown</p>	<p>None required, analysis verifies that one tip operative can safely stop rotor</p> <p>None required – shutdown occurs prior to damaging overspeed</p> <p>System changed to command shutdown prior to load dropping off. Also, backup power sensor signal sent to controller</p>
<b>Electrical power failures</b>		
<ul style="list-style-type: none"> <li>• Synchronizer provides signal to close bus tie contactor too soon or too late (WTS not proper phase relationship or voltage to mate with bus)</li> <li>• Loss of commercial power while WTS is at rated power</li> </ul>	<p>High current transient causing high torque load on the generator that could cause mechanical damage to generator or drive train</p> <p>Rotor speed increases</p>	<p>Synchronizer is fully redundant and fail safe</p> <p>None required – shutdown occurs prior to damaging overspeed</p>

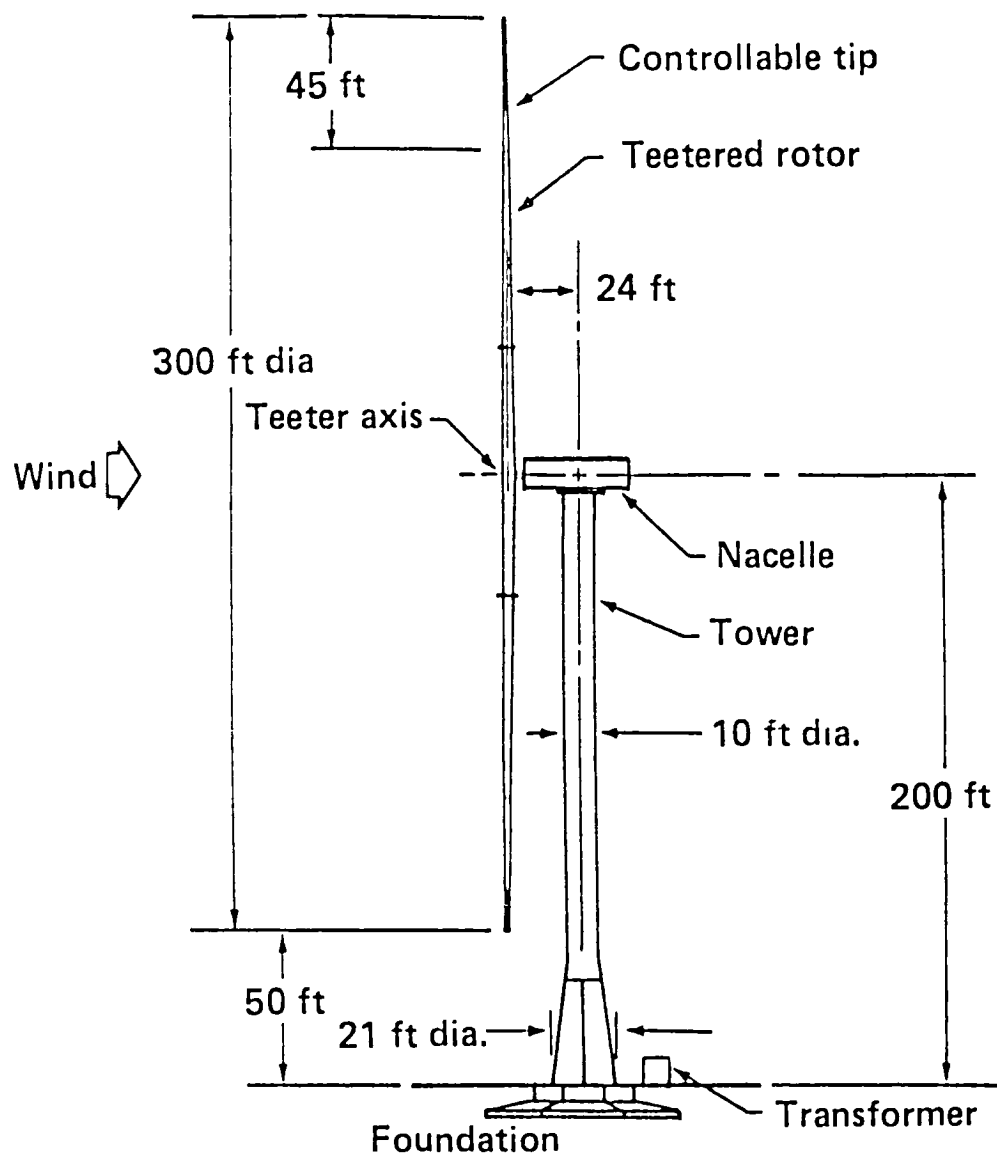


Figure 1. - Wind turbine configuration.



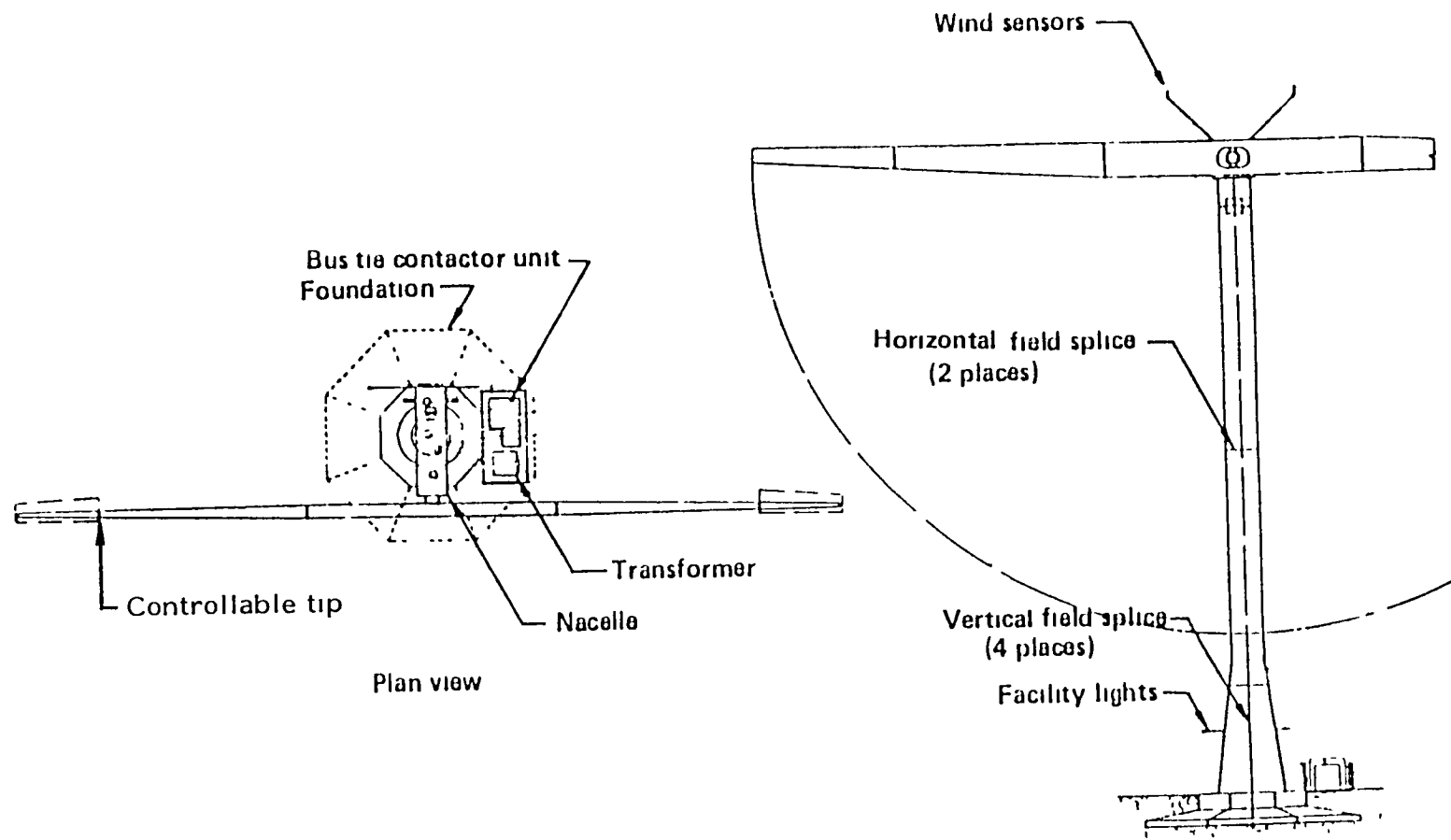


Figure 2. - Tower, foundation, and facility layout.

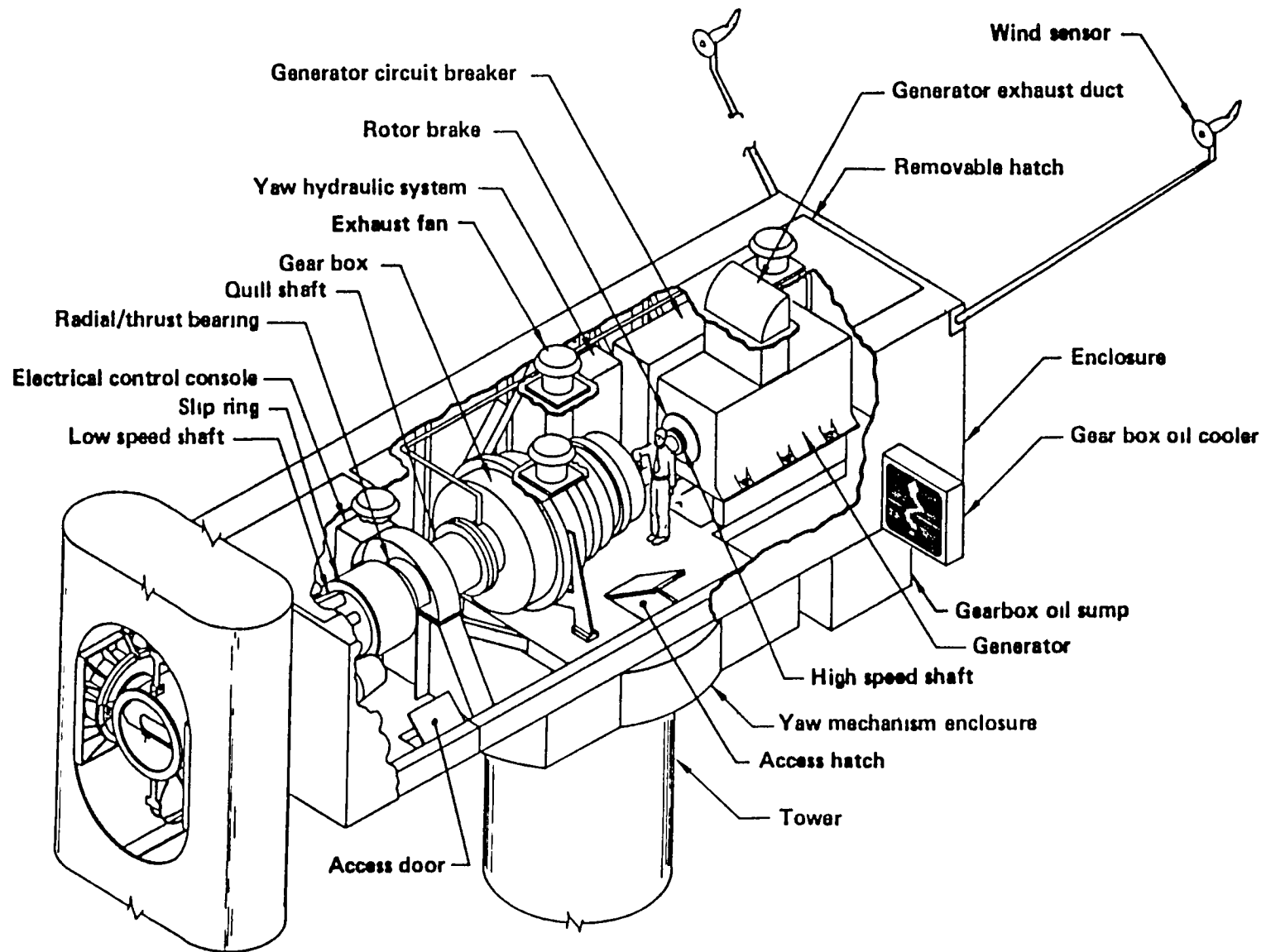


Figure 3. - Rotor and nacelle arrangement.

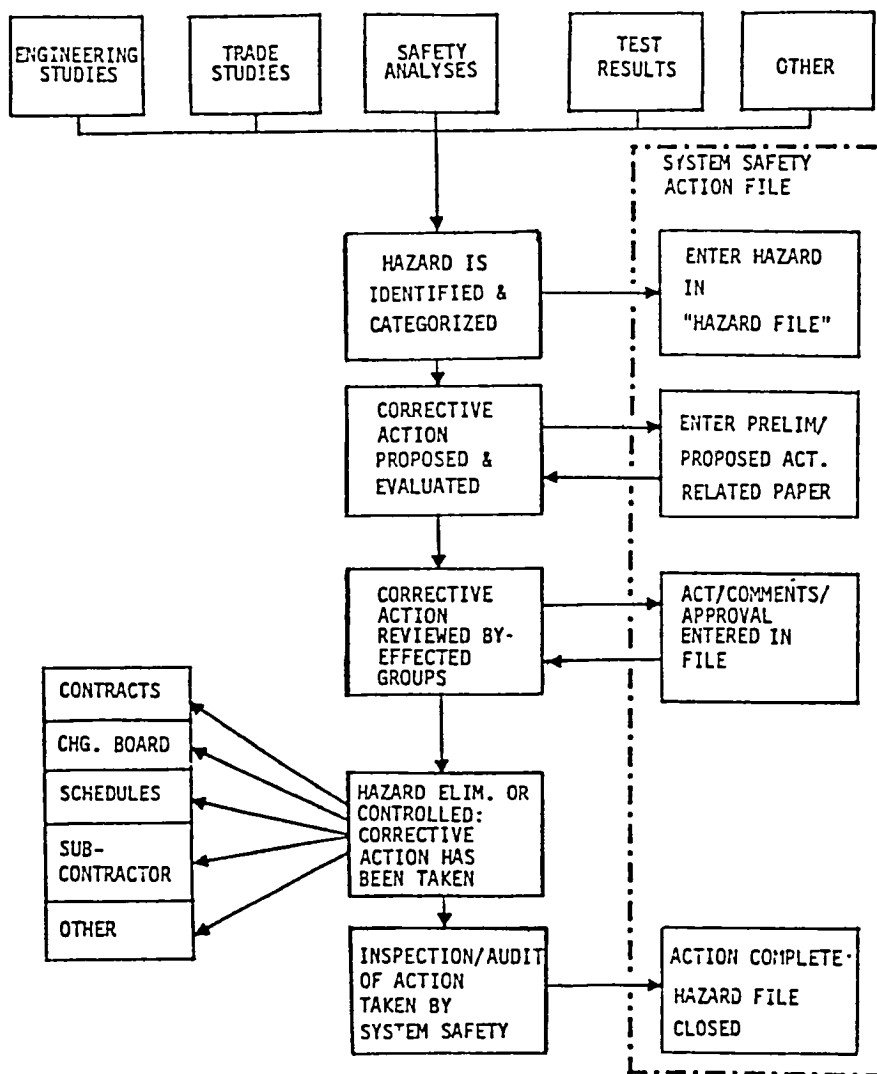


Figure 4. - Hazard corrective action loop.

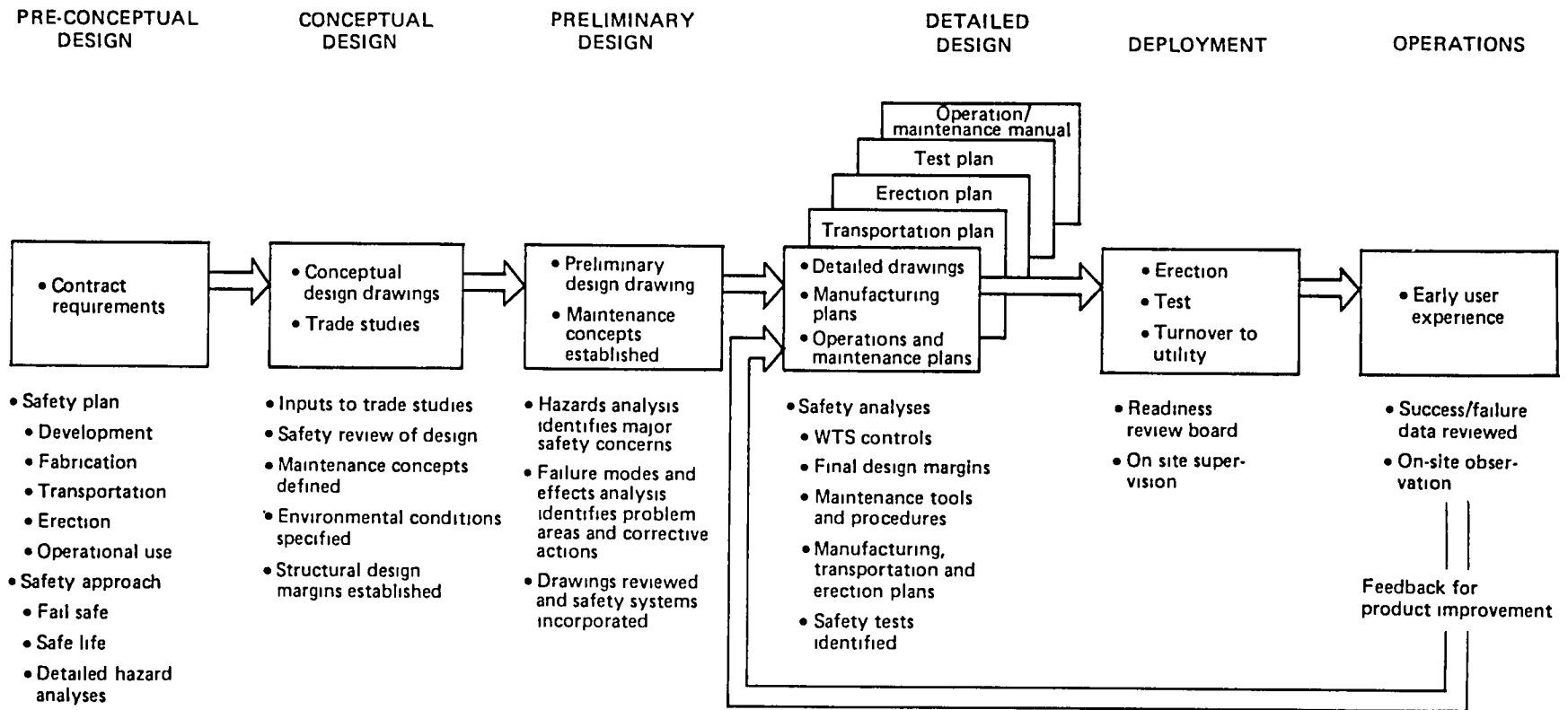


Figure 5. - Safety disciplines integrated into WTS development.

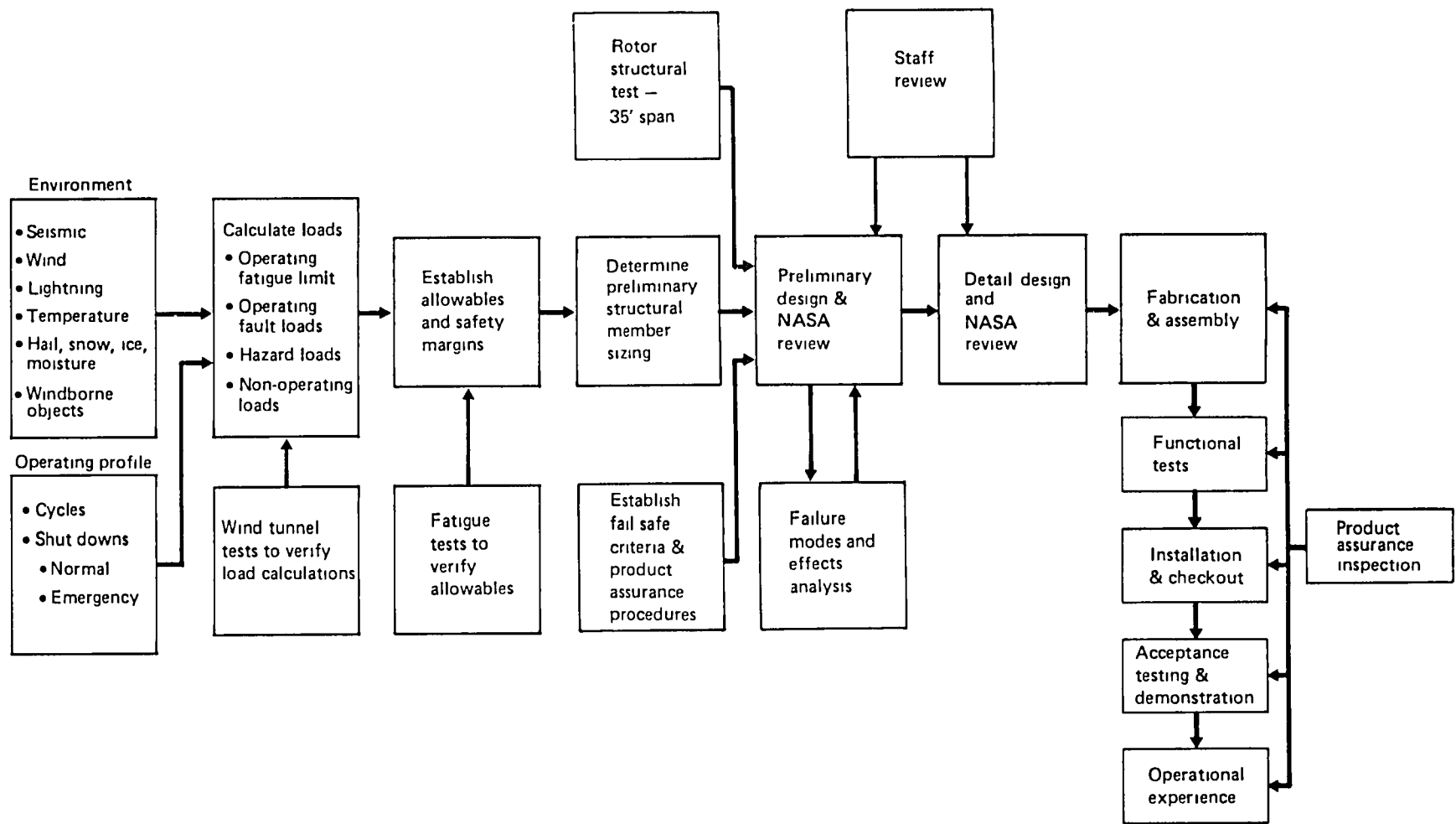


Figure 6. - MOD-2 safety assurance.

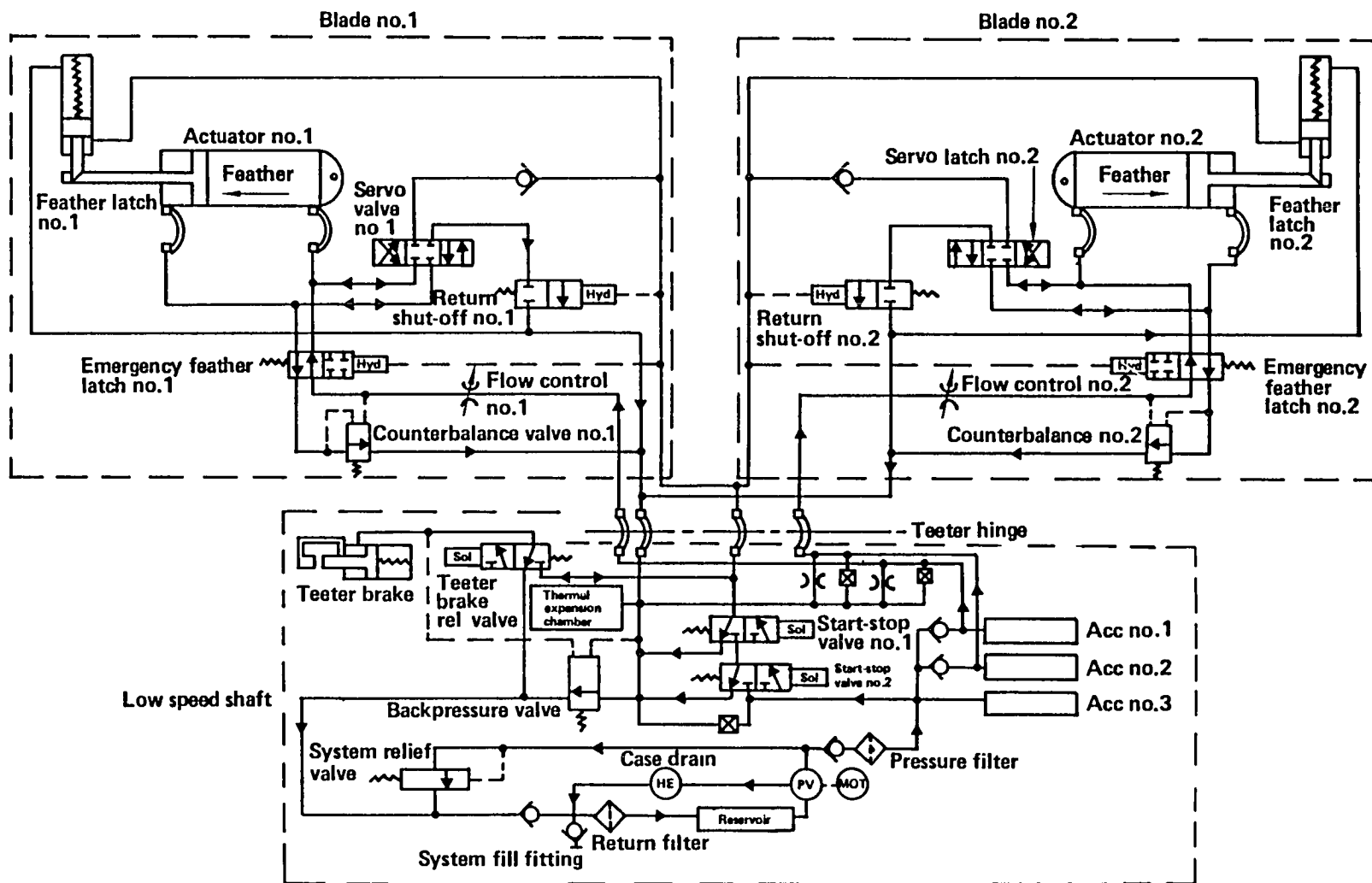
	Transportation	Storage Installation	Operational
Duration	3 weeks	3 months	30 years (2104 hr/yr standby) (6662 hr/yr pwr opn)
Wind	Negligible	Negligible	120 mph at 30 ft reference elevation
Shock	Rail: 20G peak Truck: 3G peak	Negligible	See: seismic
Vibration	3G	Negligible	As induced by the rotor, high speed shaft Gearbox
Temperature	Same as operational	Same as operational	-40°F (-40°C) to 120°F (48.9°C) ambient air
Solar radiation	Same as operational	Same as operational	363 BTU/ft <sup>2</sup> /hr, 4 hrs daily 6 months annually
Lightning	Negligible	Negligible	Variable current profile over 360 ms, with 200 kA peak current
Rain	Same as operational	Same as operational	4 inches/hour
Hail	1.0 inch dia. 50 lb/cu. ft. 132 ft/sec. vel. (applicable to shipping containers)	1.0 inch dia., 50 lb/cu. ft. 66.6 ft/sec. vel. (applicable to storage containers)	1.0 inch dia., 50 lb/cu. ft., 66.6 ft/sec vel. (horiz. & vertical surfaces)
Ice (glaze)	2.0 inches thickness, 60 lbs/cu. ft. (applicable to shipping containers)	2.0 inches thickness 60 lbs/cu. ft. (applicable to storage containers)	2.0 inches thickness, 60 lbs/cu. ft. (on all external surfaces)
Snow	41 lbs/sq. ft. (shipping containers)	41 lbs/sq. ft. (storage containers)	Blade: 21 lbs/sq. ft. Nacelle: 41 lbs/sq. ft.
Humidity, sand/ dust, salt spray, fungus	Same as operational	Same as operational	Exposure equivalent to MIL-STD-210B for exposed or sheltered ground equipment, as applicable
Fauna	Exposure to insects	Same as transportation	Same as transportation plus 4 lb. birds at 35 mph for stationary surfaces above 150 ft.
Noise	Negligible	Negligible	Negligible
Seismic	Negligible	Negligible	Site specific
Altitude	Same as operational	Same as operational	Sea level to 7000 ft.

Figure 7. - WTS design environment.

## MOD-2 Failure Mode and Effects Analysis

SUBSYSTEM		COMPONENT		PAGE 126		
TOWER - EPS		TOWER-HIGH VOLTAGE CABLE		FMEA NO 7.2.1.1		
FUNCTION OF COMPONENT						
PROVIDES A PATH FOR THE FLOW OF HIGH VOLTAGE GENERATOR OUTPUT CURRENT FROM THE CABLE TRANSITION MECHANISM TO THE HIGH VOLTAGE JUNCTION BOX AT THE FOOT OF THE TOWER.						
FAILURE MODES & EFFECTS				APPLICABLE OPERATING MODES		
1 OPEN CIRCUIT: ONE OR MORE PHASES GO TO ZERO VOLTAGE; GCB OPENS, BTC (BUSTIE CONTACTOR) OPENS, WTS SHUTS DOWN.				G		
2 SHORT CIRCUIT: POSSIBLE PHASE-TO-PHASE FAULT; GCB OPENS, BTC OPENS, WTS SHUTS DOWN.				G		
3 GROUNDED CONDUCTOR: MASSIVE FAULT ON ONE CONDUCTOR; GCB OPENS, BTC OPENS, WTS SHUTS DOWN.				G		
4						
FAILURE FREQUENCY			FAILURE SEVERITY			
FAILURE MODE NO	FAILURE MODE FREQ %	FAILURE RATE $\times 10^{-6}$ PER HOUR	MEAN TIME BETWEEN FAILURE (YEARS)	MINIMAL I	MARGINAL II	CRITICAL III
1	50	.8	286			X
2	25	.8	578			X
3	25	.8	578			X
4						
FAILURE DETECTION METHODS						
1 GENERATOR POWER INDICATION INDICATES ZERO POWER; BTC POSITION INDICATES "OPEN".						
2 -3 GENERATOR POWER INDICATION INDICATES ZERO POWER; GCB AND BTC POSITION INDICATES BOTH ARE "OPEN".						
4						
FAILURE CAUSE AND CORRECTIVE ACTION (IF APPLICABLE)						
1 DIFFERENTIAL CURRENT PROTECTION RELAY WILL CAUSE THE GCB TO OPEN OR AS A BACKUP. THE DIFFERENTIAL CURRENT PROTECTION CIRCUIT WILL CAUSE THE BTC TO OPEN.						
2 GENERATOR OR BTCU DIFFERENTIAL CURRENT PROTECTION OR GENERATOR OVER-CURRENT PROTECTION CIRCUITS WILL CAUSE THE GCB AND BTC TO OPEN						
3 SAME AS 2 PLUS THE GROUND CURRENT RELAY WILL CAUSE THE GCB TO OPEN.						
4						
OPERATING MODES				NAME G TRUSK/H ROTH		DATE 8/17/78
A - SHUTDOWN B - TRANSITION TO WARM-UP C - WARM-UP				D - TRANSITION TO STANDBY E - STANDBY F - TRANSITION TO OPERATE		G - OPERATE H - TRANSITION TO FEATHER I - FEATHER

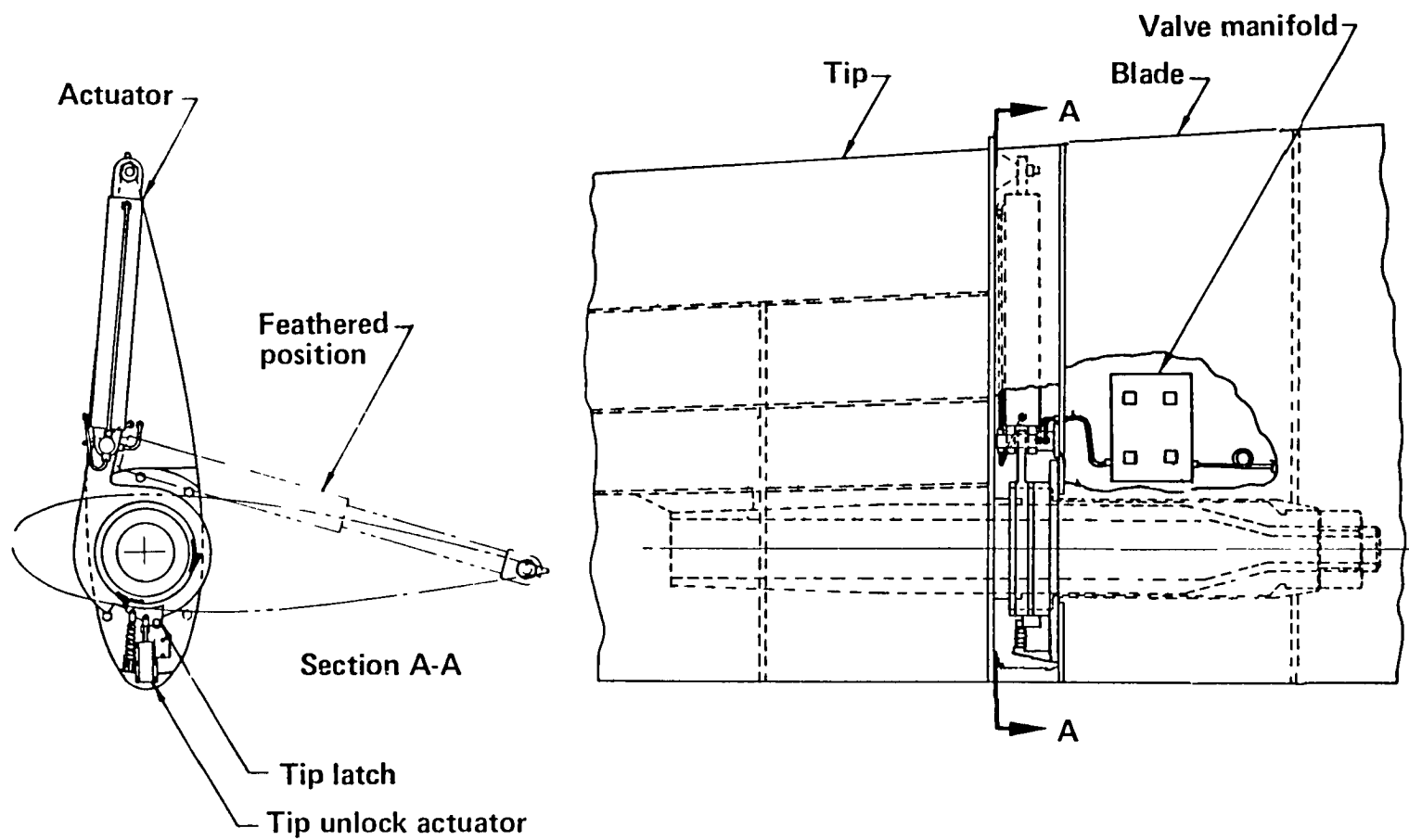
**Figure 8. - MOD-2 failure mode and effects analysis.**



(a) Hydraulic schematic pitch control system.

Figure 9. - MOD-2-107.





(b) Pitch control mechanism.

Figure 9. - Concluded.

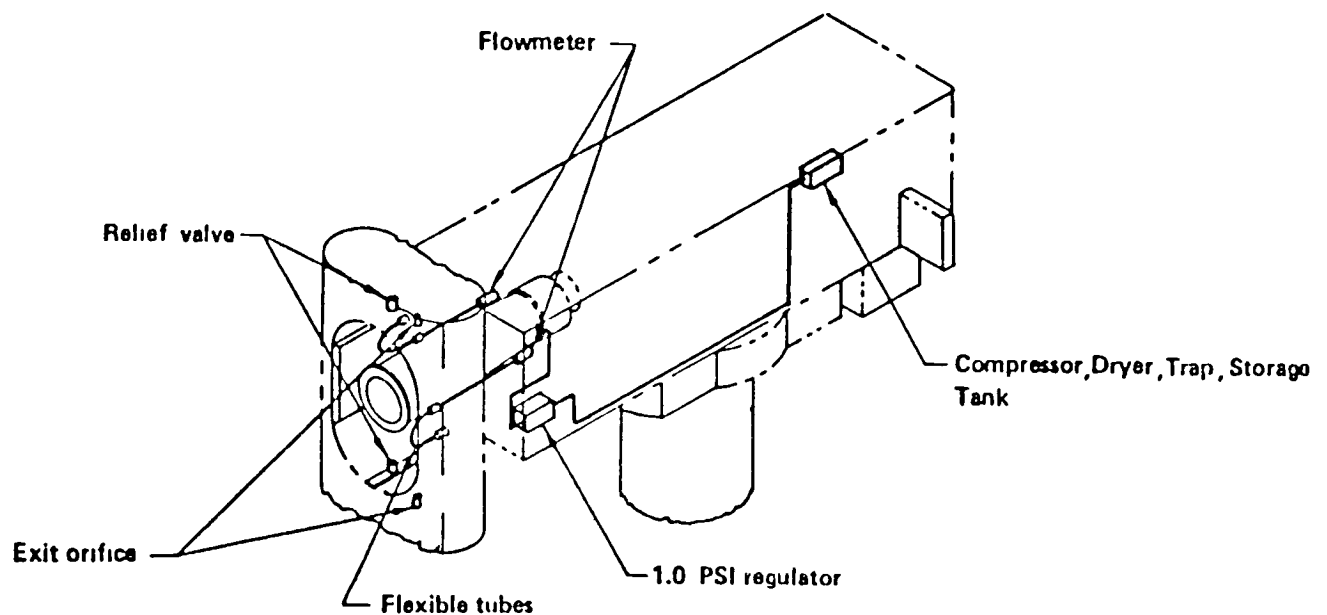
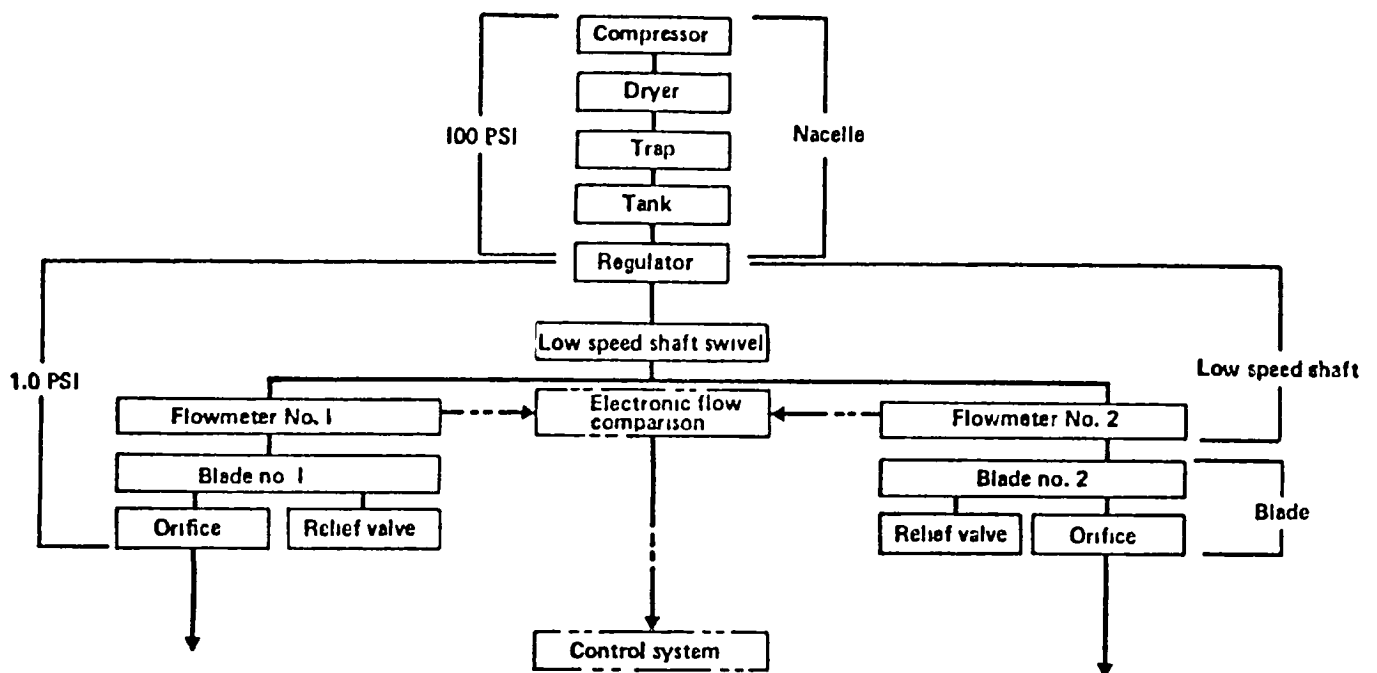


Figure 10. - Blade crack detection system.

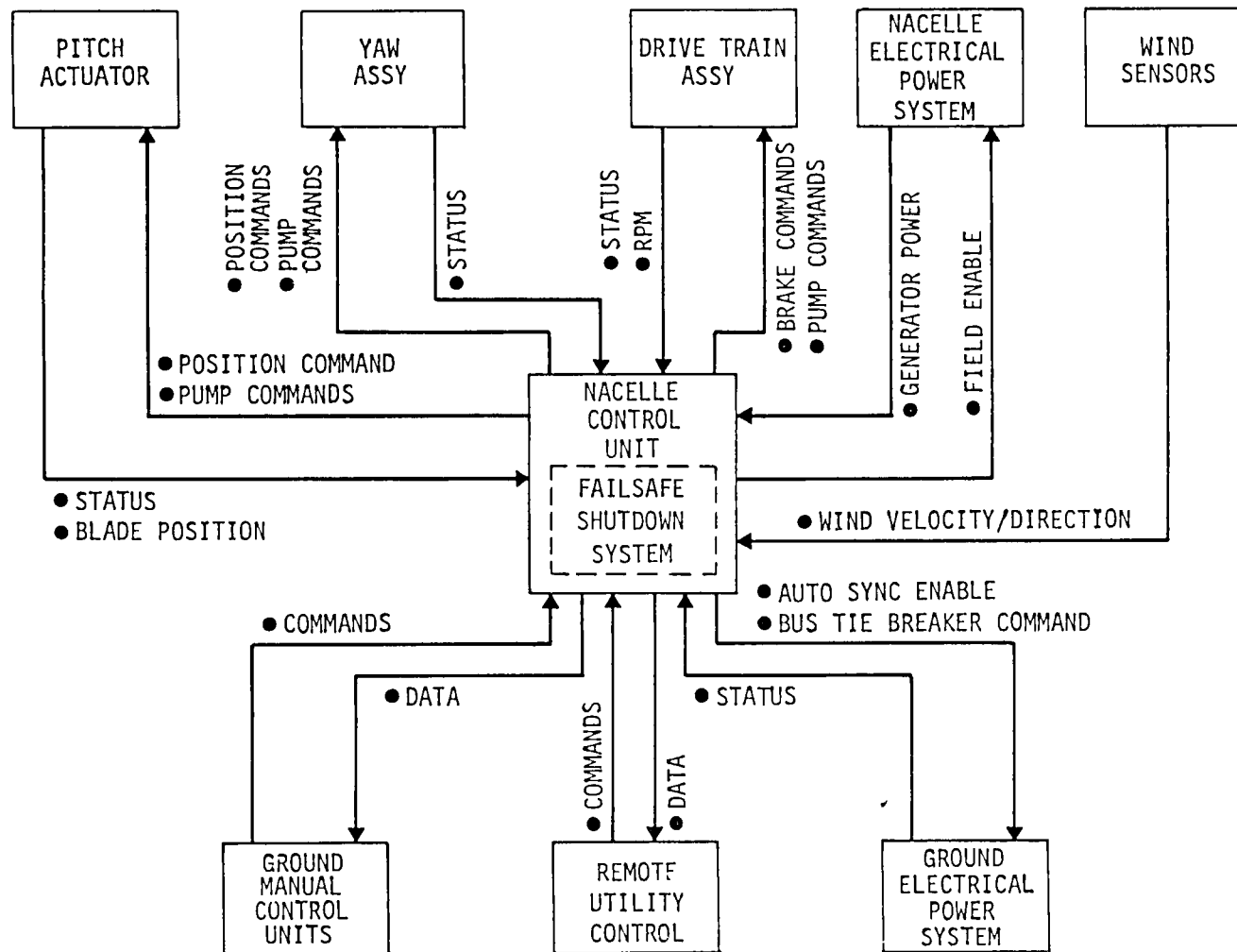


Figure 11. - Control system interface diagram.

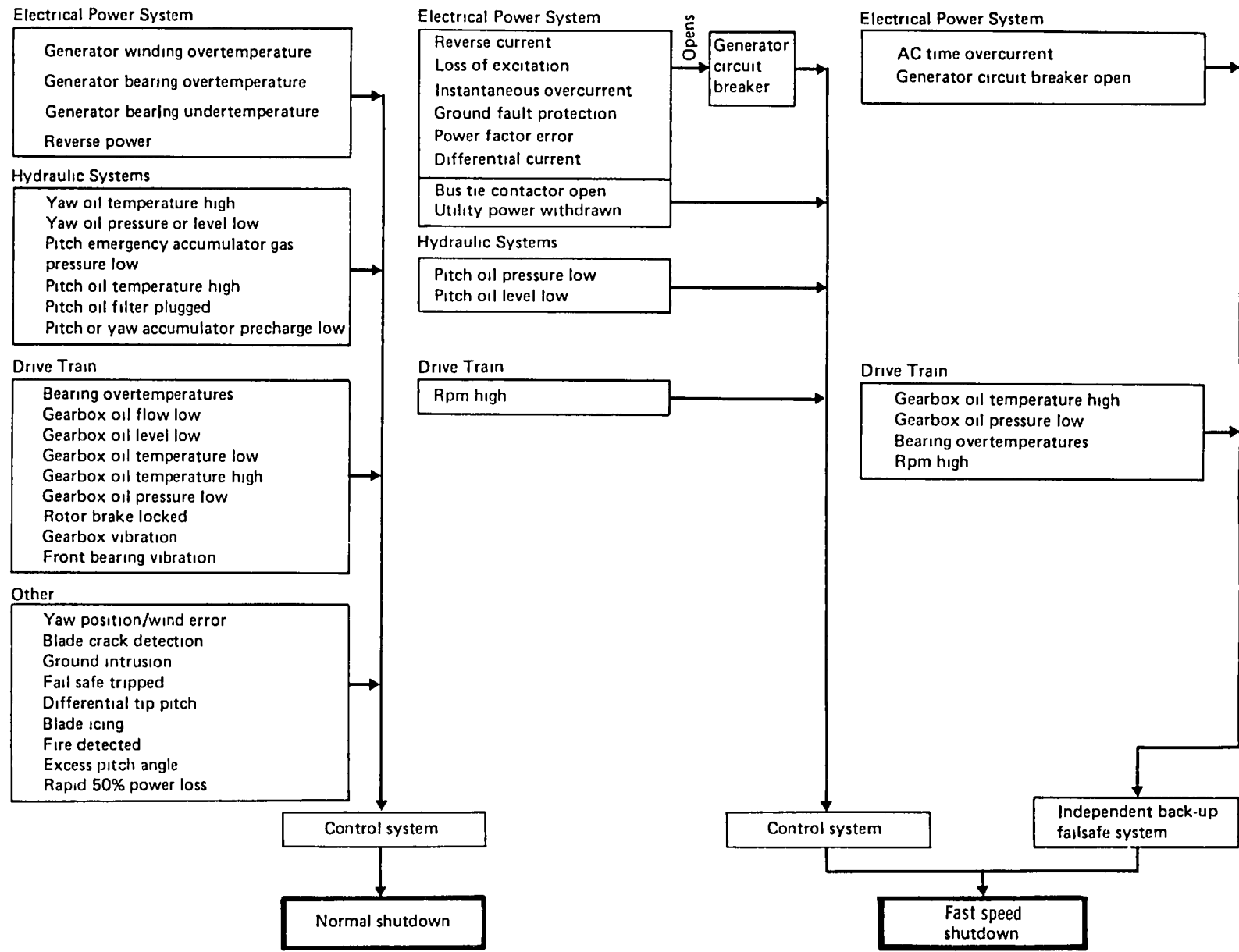


Figure 12. - MOD-2 safety system.

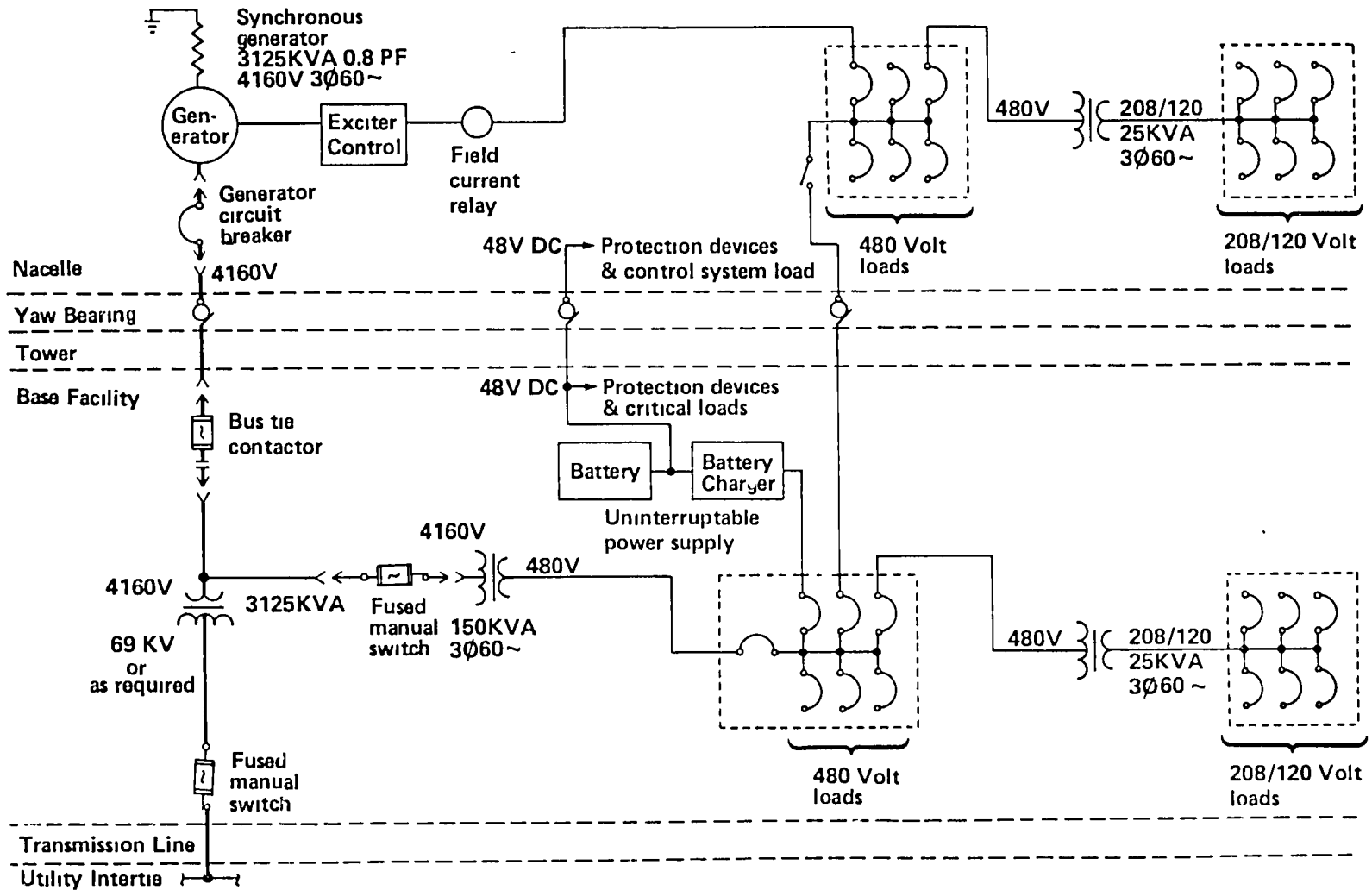


Figure 13. - Electrical system schematic.

- Failure modes and effects analysis will be conducted on all WTS elements
- All structural members "safe life" designed, all controls and electrical systems designed "fail safe"
- Occupational Safety and Health Act of 1970 (Public Law 91-596) and applicable State Safety Regulations
- MIL-STD-1472, Human Engineering Design Criteria for Military Systems, Equipment and Facilities
- IEEE Standard 142-1972, IEEE Recommended Practice for Grounding of Industrial and Commercial Power Systems
- ANSI C2 American National Standard, National Electrical Safety Code, 1977 Edition

Figure 14. - MOD-2 safety design criteria.

- Primary controls shutdown WTS upon failure; backup shutdown system, independent of control system logic and commands, protects WTS in case of control system failure
- Through electrical system protection with redundant, fail safe synchronizer and uninterruptable power supply
- Rotor crack detection system, ice detectors on blades
- Automatic fire detection and extinguishing system
- Emergency exit doors and "Rescumatic" device to allow egress from either end of Nacelle in case of uncontrolled fire
- Capability to remove person on stretcher from Nacelle
- Unauthorized entry disables WTS
- "Buddy" system used for all maintenance
- All hazardous rotating devices guarded
- Aircraft warning lights and markings per FAA regulations
- Scheduled maintenance plan to ensure integrity of safety systems

Figure 15. - MOD-2 safety system features.

1 Report No <b>NASA TM-79193</b>		2 Government Accession No		3 Recipient's Catalog No	
4 Title and Subtitle <b>SAFETY CONSIDERATIONS IN THE DESIGN AND OPERATION OF LARGE WIND TURBINES</b>				5 Report Date <b>June 1979</b>	
				6 Performing Organization Code	
7 Author(s) <b>Dwight H Reilly</b>				8 Performing Organization Report No <b>E-067</b>	
				10 Work Unit No	
9 Performing Organization Name and Address <b>National Aeronautics and Space Administration Lewis Research Center Cleveland, Ohio 44135</b>				11 Contract or Grant No	
				13 Type of Report and Period Covered <b>Technical Memorandum</b>	
12 Sponsoring Agency Name and Address <b>U.S. Department of Energy Distributed Solar Technology Division Washington, D.C. 20545</b>				14 Sponsoring Agency Code Report No <b>DOE/NASA/20305-79/3</b>	
15 Supplementary Notes <b>Final report. Prepared under Interagency Agreement DE-AI01-79ET20305</b>					
16 Abstract The engineering and safety techniques used to assure the reliable and safe operation of large wind turbine generators utilizing the Mod 2 Wind Turbine System Program as an example is described. The techniques involve a careful definition of the wind turbine's natural and operating environments, use of proven structural design criteria and analysis techniques, an evaluation of potential failure modes and hazards, and use of a fail safe and redundant component engineering philosophy. The role of an effective quality assurance program, tailored to specific hardware criticality, and the checkout and validation program developed to assure system integrity are described.					
17 Key Words (Suggested by Author(s)) <b>Wind power Safety Reliability Energy</b>			18 Distribution Statement <b>Unclassified - unlimited STAR Category 44 DOE Category UC-60</b>		
19 Security Classif (of this report) <b>Unclassified</b>		20 Security Classif (of this page) <b>Unclassified</b>		21 No of Pages	
				22 Price*	

**End of Document**